蔵野　雅昭　　前田　祐希
８７２１　　２９４６

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-006729
(43)Date of publication of application : 12.01.1996

(51)Int.Cl. G06F 3/06
G11B 19/04
G11B 20/10

(21)Application number : 06-132789
(22)Date of filing : 15.06.1994

(71)Applicant : NEC CORP
(72)Inventor : SHORIKI KEI

(54) STORAGE DEVICE WITH SECRECY PROTECTION MECHANISM AND SECRECY PROTECTION SYSTEM USING THE SAME

(57)Abstract:
PURPOSE: To protect the secrecy of stored data without manually inputting identification information by a user.
CONSTITUTION: A magnetic disk device 2 where the data are stored is freely attached to and detached from a host 12. When the power source is turned ON, a discrimination information transmission command is sent out of the disk drive 2 to the host 1. In response to the command, the stored data are allowed to be accessed only when identification information inputted from the host 1 is matched with the identification information of the disk drive. Further, the access to the data is allowed only when the identification information is inputted within a specific time clocked by a timer 27 after the identification information transmission command is sent out. If the disk device 2 is stolen, its data can not be accessed since identification information does not match or is not inputted within the specific time, so that its secrecy is protected.

LEGAL STATUS
[Date of request for examination] 15.06.1994
[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 2581008

[Date of registration] 21.11.1996

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The storage which characterizes by to include the 1st access-permission means which permits access of said data only when a command sending-out means send out an identification-information sending-out command to the external access equipment which is the storage holding the secrecy of the data which have memorized, and desorption is free and accesses self-equipment to self-equipment, and the identification information which answered this command and was inputted from said access equipment and the identification information of self-equipment are in agreement.

[Claim 2] Storage according to claim 1 characterized by including the 2nd access-permission means which permits access of said data only when it replaces with said 1st access-permission means and the input of said access equipment to identification information is in predetermined time from the time of sending out of said identification information sending-out command.

[Claim 3] It is a security-protection system in the external access equipment which desorption is free and accesses this storage to the storage holding the secrecy of the memorized data, and this storage. A command sending-out means by which said storage sends out an identification information sending-out command to said access equipment, An access-permission means to permit access of said data only when the identification information which answered this command and was inputted from said access equipment, and the identification information of a store are in agreement is included. Said access equipment is a security-protection system characterized by including an identification information sending-out means to answer said identification information sending-out command, and to send out the identification information of

self-equipment to said storage.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the security-protection system using the magnetic disk drive with a device and this holding especially the secrecy of stored data about the security-protection system which used a store with a security-protection device, and this.
[0002]
[Description of the Prior Art] There is a Provisional-Publication-No. No. 178456 [57 to] official report as a well-known technique of holding the secrecy of stored data, such as a magnetic disk drive. This permits access of a magnetic disk drive, only when identification information is in agreement. That is, identification information is beforehand recorded on the magnetic disk drive, and when a user uses a magnetic disk drive, manual input of the identification information is carried out. And the identification information beforehand recorded as the inputted identification information is collated, utilization authorization / disapproval is distinguished, and, in utilization authorization, access to a magnetic disk drive is permitted.
[0003] Moreover, the body was equipped with the key in some personal computers, in the condition of having locked, it locked electrically or the measures of preventing the theft of a magnetic disk drive physically by carrying out by the ability not disassembling a case were taken in the condition of having locked so that powering on (system startup) could not be carried out to a body.
[0004]
[Problem(s) to be Solved by the Invention] However, in the personal computer of a desktop mold, while the measures of equipping a key in the most are not taken, in order to raise operability, the attachment-and-detachment method of a magnetic disk is simplified, and possibility of encountering a theft is becoming high.
[0005] With the well-known technique of the Provisional-Publication-No. No. 178456 [57 to] official report mentioned above, there was a fault that it was necessary to input identification information manually whenever a user accesses a magnetic disk drive.
[0006] Made in order that this invention may solve the fault of the conventional technique mentioned above, the object is offering the security-protection system using the storage with a security-protection device and this which a user's does not need to input identification information manually and can hold secrecy.

[0007]
[Means for Solving the Problem] The store with a security-protection device by this invention is a store holding the secrecy of the memorized data. A command sending-out means to send out an identification information sending-out command to the external access equipment which desorption is free and accesses self-equipment to self-equipment, Only when the identification information which answered this command and was inputted from said access equipment, and the identification information of self-equipment are in agreement, it is characterized by including the 1st access-permission means which permits access of said data.
[0008] The security-protection system by this invention is a security-protection system in the external access equipment which desorption is free and accesses this storage to the storage holding the secrecy of the memorized data, and this storage. A command sending-out means by which said storage sends out an identification information sending-out command to said access equipment, An access-permission means to permit access of said data only when the identification information which answered this command and was inputted from said access equipment, and the identification information of a store are in agreement is included. It is characterized by said access equipment including an identification information sending-out means to answer said identification information sending-out command, and to send out the identification information of self-equipment to said storage.
[0009]
[Function] Access of data is permitted only when the identification information which answered the identification information command and was inputted from the external access equipment in which desorption is free, and the identification information of self-equipment are in agreement. Moreover, access of data is permitted only when the input of access equipment to identification information is in predetermined time from the time of sending out of an identification information command.
[0010]
[Example] Next, this invention is explained with reference to a drawing.
[0011] Drawing 1 is the block diagram showing the configuration of one example of the security-protection system by this invention. In drawing, the security-protection system by one example of this invention consists of a security-protection device 100 prepared in the host 1 side, and a security-protection device 200 prepared in the magnetic disk drive 2 side. In addition, the magnetic disk 20 which memorizes data at a host 1 side to a host devices [, such as a body of a personal computer,] 10 and magnetic disk drive 2 side is established, and the host 1 and magnetic disk drive 2 side is connected by the communication path 3 of a cable etc.
[0012] The security-protection device 100 by the side of a host 1 is constituted including ID storage table 13 which memorizes the original identification information (ID is called hereafter) which a user can set as arbitration, the transceiver circuit 11 which performs transmission and reception of data, and the analysis circuit 12 which

performs analysis of received data.
[0013] On the other hand, the security-protection device 200 by the side of a magnetic disk drive 2 CPU21 which supervises all the events generated within this device (Central Prosessing Unit), The transceiver circuit 22 which transmits and receives data, and the analysis circuit 23 which analyzes received data, ID storage table 24 which memorizes original ID which a user can set as arbitration, With reference to the data contained in the analyzed signal, it is constituted including the correlation circuit 25 to collate, the control circuit 26 which performs reservation/cutting control of the communication path of a magnetic disk drive 2 and a host 1, and the timer 27 which supervises the time amount which the user set as arbitration.
[0014] In this configuration, the user registers original ID of arbitration into ID storage tables 13 and 24 beforehand. In this case, the same ID information is registered into ID storage tables 13 and 24.
[0015] Generally, although CPU within the body in a personal computer performs initialization processing to the magnetic disk drive connected to the power up to a body, it performs distinction just as a connection partner, or unjust from a magnetic disk drive 2 side to a host 1 side in this initialization processing in the system of this example.
[0016] By the security-protection device 200 prepared in the magnetic disk drive 2 side, the data used as the instruction for making ID answer a letter are sent from the transceiver circuit 22 to the security-protection device 100 prepared in the host 1 side based on the instruction of CPU21.
[0017] In the security-protection device 100, the transceiver circuit 11 receives the data sent from the transceiver circuit 22, and it analyzes in the analysis circuit 12. And the data containing the ID are generated with reference to ID registered into ID storage table 13 based on the analyzed content, and a letter is answered from the transceiver circuit 11.
[0018] Next, by the security-protection device 200, the data answered from the security-protection device 100 are received in the transceiver circuit 22, and reply data are analyzed in the analysis circuit 23. And ID contained in the data analyzed in the analysis circuit 23, i.e., ID registered into ID storage table 13, and ID registered into ID storage table 24 are set and collated [compare and] with a correlation circuit 25.
[0019] When ID is in agreement as a result of collating, it is judged that it is a connection request from a just host. In this case, the data which mean connection authorization are sent to the security-protection device 100, and a communication path with a magnetic disk 20 is secured by the control circuit 26. Thereby, processing is ended. It is not necessary to input ID henceforth and it can access a magnetic disk 20 as usual.
[0020] On the other hand, when ID is not in agreement as a result of collating, it is

judged as the connection request from an unspecified host, and, as for a control circuit 26, a communication path with the security-protection device 100 is cut electrically. Thereby, processing is ended.
[0021] Moreover, the timer 27 is constituted so that a user can set up the time amount of arbitration. And when the security-protection device 200 sends out the data used as the instruction for making ID answer a letter, if there is no reply of the security-protection device 100 to ID into the setup time of the timer [from] 27, it will be judged as the connection request from an unspecified host, and a control circuit 26 will cut electrically a communication path with the security-protection device 100. Thereby, processing is ended. In addition, a key input, the switch on the tooth back of equipment, etc. perform time setting to a timer 27. Time amount may be set up beforehand.
[0022] By equipping the monitoring function by the timer 27 the security-protection device 100 and whose security-protection device 200 are what becomes a pair and functions fundamentally, when a magnetic disk includes a third party's hand according to a theft etc., the secrecy of data can be held. That is, since there is no reply of ID into the setup time of a timer 27 when the security-protection device 100 is not formed in a third party's host side, it can become a time-out, and can judge that it is a connection request from an unspecified person's host, and a communication path can be electrically cut to the connection request from an unspecified host.
[0023] Although possibility that equipment will encounter a theft is also becoming high with the miniaturization of a magnetic disk drive in recent years, and simplification of an attachment-and-detachment method, it is avoidable that the data memorized even if it should encounter a theft according to the equipment of this example flow out outside. When the data memorized are extra sensitive information, it is thought that especially this magnetic disk drive is effective.
[0024] As mentioned above, the data memorized even if a store is in a theft by permitting access, only when ID is in agreement are not accessed, and the secrecy of the data can be held. And the user does not need to input ID.
[0025] Also when the input of ID is in predetermined time from a power up and it permits access, similarly data are not accessed and the secrecy can be held.
[0026] In addition, although the case of a magnetic disk drive was made into the example and the above example explained, it is clear that this invention can apply to various kinds of storage, such as not only this but a semiconductor memory, widely.
[0027] In relation to the publication of a claim, this invention can take the following mode further.
[0028] (1) Said command sending-out means is storage according to claim 1 or 2 characterized by sending out said identification information sending-out command to the power up of self-equipment.
[0029] (2) Said command sending-out means is storage according to claim 1 or 2 characterized by sending out said identification information sending-out command at

the time of initialization of self-equipment.
[0030] (3) Said command sending-out means is a security-protection system according to claim 3 characterized by sending out said identification information sending-out command to the power up of said storage.
[0031] (4) Said command sending-out means is a security-protection system according to claim 3 characterized by sending out said identification information sending-out command at the time of initialization of said storage.
[0032]
[Effect of the Invention] Access of data is permitted only when the identification information which this invention answered the identification information command and was inputted from external access equipment, and the identification information of a store are in agreement, as explained above. Moreover, only when the input of access equipment to identification information is in predetermined time from the time of sending out of an identification information command, by permitting access of data, it is effective in the ability to hold the secrecy of the data held at the store.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the block diagram showing the security-protection structure of a system by the example of this invention.
[Description of Notations]
1 Host
2 Magnetic Disk Drive
3 Communication Path
10 Host Device
20 Magnetic Disk
11 22 Transceiver circuit
12 23 Analysis circuit
13 24 ID storage table
21 CPU
25 Correlation Circuit
26 Control Circuit
27 Timer
100,200 Security-protection device

---

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－6729

(43)公開日　平成８年(1996)１月12日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	3/06	３０１	Ｚ		
Ｇ１１Ｂ	19/04	５０１	Ｈ	7525－5D	
	20/10		Ｈ	7736－5D	

審査請求　有　　請求項の数３　ＯＬ　（全　４　頁）

(21)出願番号　特願平6－132789

(22)出願日　平成６年(1994)６月15日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　正力　慶
東京都港区芝五丁目７番１号　日本電気株式会社内

(74)代理人　弁理士　▲柳▼川　信

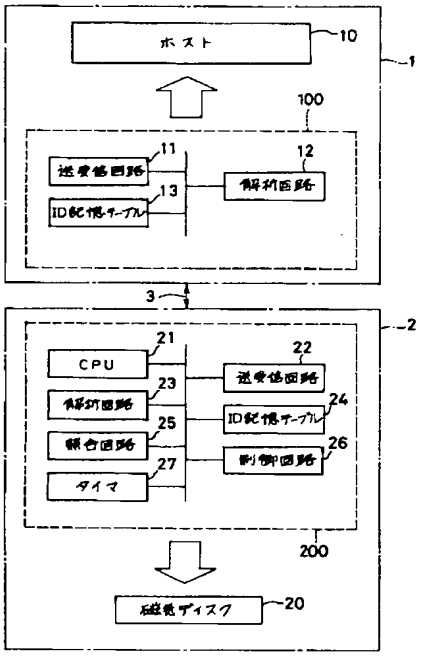
(54)【発明の名称】　機密保持機構付き記憶装置及びこれを用いた機密保持システム

(57)【要約】

【目的】　利用者が識別情報を手動入力する必要なく、記憶されているデータの機密を保持する。

【構成】　データを記憶している磁気ディスク装置２は、ホスト１２に対して脱着自在である。電源投入時に、ディスク装置２からホスト１に対し識別情報送出指令を送出する。この指令に応答してホスト１から入力された識別情報とディスク装置の識別情報とが一致したときにのみ記憶されているデータのアクセスを許可する。また、識別情報送出指令の送出時からタイマ２７による所定時間内に識別情報が入力された場合にのみデータのアクセスを許可する。

【効果】　ディスク装置２が盗難に遭った場合には、識別情報が一致しない又は識別情報が所定時間内に入力されないので、データをアクセスできず、その機密を保持できる。



【特許請求の範囲】
【請求項１】　記憶しているデータの機密を保持する記憶装置であって、自装置に対して脱着自在でありかつ自装置をアクセスする外部アクセス装置に対し識別情報送出指令を送出する指令送出手段と、この指令に応答して前記アクセス装置から入力された識別情報と自装置の識別情報とが一致したときにのみ前記データのアクセスを許可する第１のアクセス許可手段とを含むことを特徴とする記憶装置。
【請求項２】　前記第１のアクセス許可手段に代えて、前記識別情報送出指令の送出時から所定時間内に前記アクセス装置から識別情報の入力があったときにのみ前記データのアクセスを許可する第２のアクセス許可手段を含むことを特徴とする請求項１記載の記憶装置。
【請求項３】　記憶しているデータの機密を保持する記憶装置とこの記憶装置に対して脱着自在であり該記憶装置をアクセスする外部アクセス装置とにおける機密保持システムであって、前記記憶装置は前記アクセス装置に対し識別情報送出指令を送出する指令送出手段と、この指令に応答して前記アクセス装置から入力された識別情報と記憶装置の識別情報とが一致したときにのみ前記データのアクセスを許可するアクセス許可手段とを含み、前記アクセス装置は前記識別情報送出指令に応答して自装置の識別情報を前記記憶装置に対して送出する識別情報送出手段を含むことを特徴とする機密保持システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は機密保持機構付き記憶装置及びこれを用いた機密保持システムに関し、特に記憶データの機密を保持する機構付きの磁気ディスク装置及びこれを用いた機密保持システムに関する。
【０００２】
【従来の技術】磁気ディスク装置等の記憶データの機密を保持する公知技術として特開昭５７－１７８４５６号公報がある。これは識別情報同士が一致したときにのみ磁気ディスク装置のアクセスを許可するものである。すなわち、予め磁気ディスク装置に識別情報を記録しておき、利用者が磁気ディスク装置を利用する場合には識別情報を手動入力させる。そして、その入力された識別情報と予め記録された識別情報とを照合して利用許可／不許可を判別し、利用許可の場合においてのみ磁気ディスク装置へのアクセスを許可するものである。
【０００３】また、一部のパーソナルコンピュータでは本体に鍵を装備し、鍵を掛けた状態では本体に電源投入（システム起動）できないように電気的にロックしたり、あるいは鍵を掛けた状態では筐体を解体できなくすることで物理的に磁気ディスク装置の盗難を防止する等の対策が施されていた。
【０００４】
【発明が解決しようとする課題】しかし、デスクトップ型のパーソナルコンピュータではそのほとんどにおいて鍵を装備するといった対策が施されていない一方で、操作性を向上させるために磁気ディスクの着脱方式が簡易化されてきており、盗難に遭う可能性が高くなってきている。
【０００５】上述した特開昭５７－１７８４５６号公報の公知技術では利用者が磁気ディスク装置をアクセスする度に識別情報を手動入力する必要があるという欠点があった。
【０００６】本発明は上述した従来技術の欠点を解決するためになされたものであり、その目的は利用者が識別情報を手動入力する必要なく機密を保持することのできる機密保持機構付き記憶装置及びこれを用いた機密保持システムを提供することである。
【０００７】
【課題を解決するための手段】本発明による機密保持機構付き記憶装置は、記憶しているデータの機密を保持する記憶装置であって、自装置に対して脱着自在でありかつ自装置をアクセスする外部アクセス装置に対し識別情報送出指令を送出する指令送出手段と、この指令に応答して前記アクセス装置から入力された識別情報と自装置の識別情報とが一致したときにのみ前記データのアクセスを許可する第１のアクセス許可手段とを含むことを特徴とする。
【０００８】本発明による機密保持システムは、記憶しているデータの機密を保持する記憶装置とこの記憶装置に対して脱着自在であり該記憶装置をアクセスする外部アクセス装置とにおける機密保持システムであって、前記記憶装置は前記アクセス装置に対し識別情報送出指令を送出する指令送出手段と、この指令に応答して前記アクセス装置から入力された識別情報と記憶装置の識別情報とが一致したときにのみ前記データのアクセスを許可するアクセス許可手段とを含み、前記アクセス装置は前記識別情報送出指令に応答して自装置の識別情報を前記記憶装置に対して送出する識別情報送出手段を含むことを特徴とする。
【０００９】
【作用】識別情報指令に応答して脱着自在な外部アクセス装置から入力された識別情報と自装置の識別情報とが一致したときにのみデータのアクセスを許可する。また、識別情報指令の送出時から所定時間内にアクセス装置から識別情報の入力があったときにのみデータのアクセスを許可する。
【００１０】
【実施例】次に、本発明について図面を参照して説明する。
【００１１】図１は本発明による機密保持システムの一実施例の構成を示すブロック図である。図において、本発明の一実施例による機密保持システムは、ホスト１側に設けられた機密保持機構１００と、磁気ディスク装置

２側に設けられた機密保持機構２００とから構成される。なお、ホスト１側にはパーソナルコンピュータ本体等のホスト機構１０、磁気ディスク装置２側にはデータを記憶する磁気ディスク機構２０が設けられ、ホスト１側と磁気ディスク装置２側とがケーブル等の通信経路３で接続されている。

【００１２】ホスト１側の機密保持機構１００は、利用者が任意に設定可能な独自の識別情報（以下、ＩＤと称する）を記憶するＩＤ記憶テーブル１３と、データの送受信を行う送受信回路１１と、受信データの解析を行う解析回路１２とを含んで構成されている。

【００１３】一方、磁気ディスク装置２側の機密保持機構２００は、本機構内で発生する全ての事象を監視するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｓｅｓｓｉｎｇ　Ｕｎｉｔ）２１と、データの送受信を行う送受信回路２２と、受信データを解析する解析回路２３と、利用者が任意に設定可能な独自のＩＤを記憶するＩＤ記憶テーブル２４と、解析した信号に含まれるデータを参照、照合する照合回路２５と、磁気ディスク装置２とホスト１との通信経路の確保／切断制御を実行する制御回路２６と、利用者が任意に設定した時間を監視するタイマ２７とを含んで構成されている。

【００１４】かかる構成において、利用者はＩＤ記憶テーブル１３及び２４に任意の独自のＩＤを予め登録しておく。この場合、ＩＤ記憶テーブル１３及び２４には同一のＩＤ情報を登録しておく。

【００１５】一般にパーソナルコンピュータにおける本体内のＣＰＵは、本体への電源投入時に接続されている磁気ディスク装置に対してイニシャライズ処理を実行するが、本例のシステムではこのイニシャライズ処理の中で磁気ディスク装置２側からホスト１側に対して接続相手として正当であるか不当であるかの判別を行う。

【００１６】磁気ディスク装置２側に設けられた機密保持機構２００では、ＣＰＵ２１の命令に基づきホスト１側に設けられた機密保持機構１００に対し、ＩＤを返信させるための命令となるデータを送受信回路２２より発信する。

【００１７】機密保持機構１００においては、送受信回路２２から発信されたデータを送受信回路１１により受信し、解析回路１２にて解析を行う。そして、解析した内容に基づいてＩＤ記憶テーブル１３に登録されているＩＤを参照し、そのＩＤを含むデータを生成して送受信回路１１から返信する。

【００１８】次に、機密保持機構２００では、機密保持機構１００から返信されてきたデータを送受信回路２２にて受信し、解析回路２３にて返信データの解析を行う。そして、解析回路２３にて解析したデータに含まれているＩＤ、すなわちＩＤ記憶テーブル１３に登録されているＩＤとＩＤ記憶テーブル２４に登録されているＩＤとを照合回路２５において比較、照合する。

【００１９】照合の結果ＩＤ同士が一致した場合は、正当なホストからの接続要求であると判断する。この場合は、接続許可を意味するデータを機密保持機構１００に対して発信し、制御回路２６により磁気ディスク機構２０との通信経路を確保する。これにより処理が終了となる。以後はＩＤを入力する必要はなく、通常どおり磁気ディスク機構２０をアクセスすることができる。

【００２０】一方、照合の結果ＩＤ同士が一致しない場合は、不特定ホストからの接続要求と判断し、制御回路２６は機密保持機構１００との通信経路を電気的に切断する。これにより処理が終了となる。

【００２１】また、タイマ２７は利用者が任意の時間を設定できるように構成されている。そして、ＩＤを返信させるための命令となるデータを機密保持機構２００が送出した時からタイマ２７の設定時間内に機密保持機構１００からＩＤの返信がなければ、不特定ホストからの接続要求と判断し、制御回路２６は機密保持機構１００との通信経路を電気的に切断する。これにより、処理が終了となる。なお、タイマ２７への時間設定は、キー入力や装置背面のスイッチ等により行う。予め時間が設定されていても良い。

【００２２】機密保持機構１００と機密保持機構２００とは基本的には対になって機能するものであるタイマ２７による監視機能を装備することにより、盗難等により第三者の手に磁気ディスクが渡った場合においてもデータの機密を保持することができる。すなわち、第三者のホスト側に機密保持機構１００が設けられていない場合には、タイマ２７の設定時間内にＩＤの返信がないため、タイムアウトとなり不特定者のホストからの接続要求であると判断し、不特定ホストからの接続要求に対し通信経路を電気的に切断することができる。

【００２３】近年の磁気ディスク装置の小型化、着脱方式の簡易化に伴い、装置が盗難に遭う可能性も高くなってきたが、本例の装置によれば万が一盗難に遭っても記憶されているデータが外部に流出することを回避することができる。記憶されているデータが機密情報である場合に、本磁気ディスク装置は特に効果があるものと考えられる。

【００２４】以上のように、ＩＤ同士が一致した場合にのみアクセスを許可することにより、たとえ記憶装置が盗難にあっても記憶されているデータをアクセスされることはなく、そのデータの機密を保持できるのである。しかも、利用者はＩＤを入力する必要がないのである。

【００２５】電源投入時から所定時間内にＩＤの入力があったときにのみアクセスを許可する場合も同様にデータをアクセスされることはなく、その機密を保持できるのである。

【００２６】なお、以上の実施例では磁気ディスク装置の場合を例にして説明したが、これに限らず半導体記憶装置等各種の記憶装置に本発明が広く適用できることは